Thinstuff LX Server
Version 1.2

User Manual

www.**thinstuff**.com

Table of Contents

1 Overview 4
1.1 Important Concepts 4
1.1.1 Connections and Sessions 4
1.1.2 Profiles 4
1.1.3 Settings 4
1.1.4 Rights 5
1.1.5 Joining sessions (shadowing) 5
1.2 Parts 6
2 Installation 7
2.1 Introduction 7
2.2 Installation layout 7
2.3 Installation steps 8
2.3.1 Restore 8
2.3.2 Install 8
2.3.3 Upgrade 8
2.3.4 Remove 9
2.3.5 Exit 9
2.4 First Steps 9
2.4.1 Evaluation Mode 9
2.4.2 Licenses 9
2.4.3 Users 10
2.4.4 Session Type 10
2.4.5 Starting the server at system startup 10
2.5 Automating the installation process 11
2.6 Important files and directories 11
2.7 Making manual backups 12
3 Web interface 13
3.1 Server Status 13
3.1.1 Server Health 13
3.1.2 License Info 14
3.2 Sessions 15
3.3 Rights 15
3.3.1 Users 16
3.3.2 Groups 17
3.4 Settings 17
3.4.1 Global Settings 18
3.4.2 Profiles 18
3.4.3 Settings Wizard 20
3.4.4 Advanced Settings 20
3.4.5 Default Settings 22
4 Session startup 23
4.1 Connection setup and authentication 23

© 2006-2007 Thinstuff s.r.o

http://www.thinstuff.com

4.2 Session setup 24
5 Internationalization and Localization 25
5.1 Language 26
5.2 Keyboard Layout 26
5.3 Caveats 26
6 Joining sessions (shadowing) 27
7 Virtual Channels 28
8 Advanced configuration 28
8.1 Database configuration 28
8.2 Web server configuration 28
8.3 Command-line client 29
8.3.1 Return codes and command input/output 29
8.3.2 Starting the command line client 30
8.3.3 Command line options 30
8.3.4 Datasets 31
9 Licensing, Upgrading and Support 35
9.1 Licensing 35
9.2 Upgrading 36
10 How-to 36
10.1 Profile Questions 36
10.2 Session Questions 37
10.3 Authentication Questions 38
10.4 Virtual Channel Questions 39
11 Compatibility 39
11.1 RDP Clients 39
11.2 Hardware and Software 40
12 Trademarks 40
Appendix A – Settings Descriptions 41

© 2006-2007 Thinstuff s.r.o

1 Overview

This chapter will give you a basic overview about the operation of the Thinstuff LX Server. If you are already familiar with the server you can skip right ahead to chapter 2 for instructions on how to install or upgrade the server.

1.1 Important Concepts

These chapters explain a few important concepts of Thinstuff LX Server to help you understand the rest of the documentation.

1.1.1 Connections and Sessions

A session is a graphical desktop running on Thinstuff LX Server. Usually a session is viewed by exactly one connection, but under certain circumstances (e.g. shadowing) more connections can view the same session at the same time.

It may happen that a session is not viewed by anyone. In this case it still continues to exist (and programs running in the session will continue to work normally). Such sessions can later receive new connections so that it is possible to continue working with them.

The login screen you see when you connect to the server is also a session. This is a special case however, since it does not run with privileges of your user (since it does not know who you are yet), but under the privileges of a special login user.

When a session is destroyed (manually, or because the program for this session ends) then all connections for this session are automatically destroyed. On the contrary, destroying a connection does not destroy the associated session automatically.

Sometimes the Thinstuff LX Server creates connections and sessions for its internal use (for example during the login process). These sessions and connections do not count against your license limit but do otherwise work normally.

1.1.2 Profiles

In addition to being associated with a specific user, a session is also associated with a specific profile. Profiles are a way of determining settings for sessions based on the user, group or host you connect from. This means that although you login with the same username, you might receive different settings when connecting from the office or from home, for example.

1.1.3 Settings

Settings specify operational parameters of the Thinstuff LX Server. These include everything from maximum allowed color depth to fine-tuning the RDP protocol

© 2006-2007 Thinstuff s.r.o

itself. Individual settings and how to use them to achieve certain setups are covered in chapters 3.4 and Appendix A.

1.1.4 Rights

Rights are similar to settings, but instead of being based on profiles they are based on users and groups. Rights handle questions of what a specific user is allowed or denied to do. Like permissions of file systems, rights are organized hierarchically. Chapter 3.3.1 explains in more detail how rights of users and groups are combined to form the final rights of a user.

1.1.5 Joining sessions (shadowing)

As mentioned in chapter 1.1.1, a session can be viewed by more than one connection. This process is usually called shadowing. Unlike a Windows RDP Server, Thinstuff LX Server allows an arbitrary number of connections to view a session. Because our "shadowing" allows much more things then just watching a copy of someone else's desktop we call this process "Joining a Session". In the rest of this document joining and shadowing is used interchangeably.

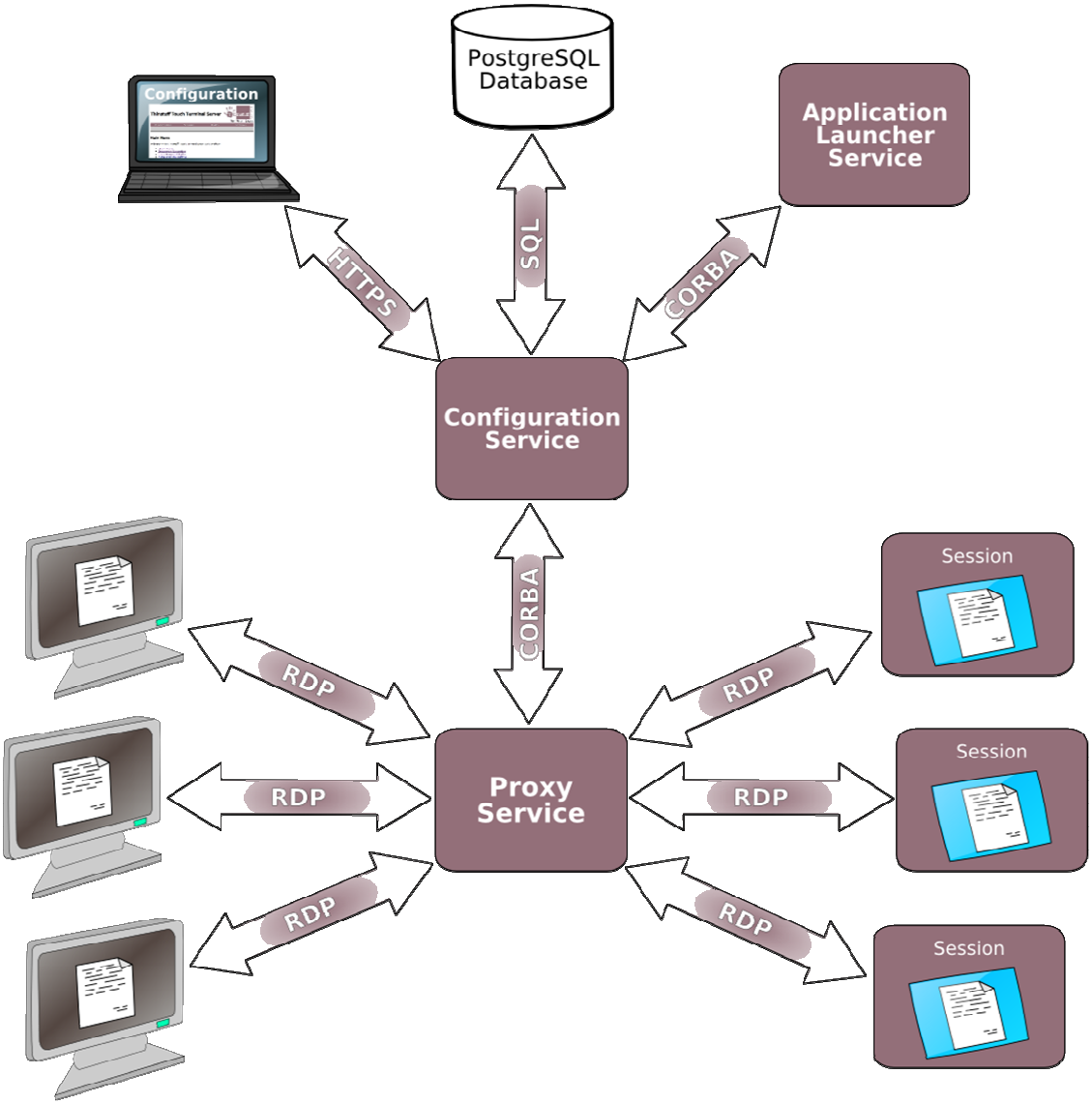
When you join a session, your connection is disconnected from the old session, and you are connected to the new session. You could basically achieve the same result by disconnecting your client and connecting again to the new session. Let's use an example to illustrate this. Assume that you have a permanent session on the server where your mail program runs and a second session where you perform your normal work. If you have a connection to your work session open and want to view mail, you have three options:

- Open a second connection and connect to the mail session
- Disconnect from the work session and connect to the mail session
- Join the mail session, which effectively behaves like the disconnect option.

Now, assume you joined the mail session and then leave for home without disconnecting. On a Windows server both your sessions would be blocked. You cannot connect to the work session because it is shadowing something else, and you cannot connect to the mail session because it is already being shadowed. If you want to use any of the sessions, then you have to force the client you left on in the office to disconnect. On Thinstuff LX Servers you can work with both sessions without any problems. The work session will show as disconnected (since its connection moved over to the mail session) and the mail session will show one connection (from the office) but since any number of connections can join a session this is not a problem at all.

© 2006-2007 Thinstuff s.r.o

1.2 Parts



As indicated by the illustration, Thinstuff LX Server consists of six parts:

1. **The proxy service**. As far as the RDP client is concerned, this is the server. All connection requests are handled by it, and then internally forwarded to the appropriate services. If this service is shut down, all connected clients will lose their connection and no new connections are possible until the service is restarted. This does not influence the actual sessions however. Once the service is restarted, client can reconnect to their respective sessions.
2. **The application launcher service**. This service starts applications (e.g. sessions) on behalf of the Thinstuff LX Server. It makes sure that all processes launched are running under the correct user and permissions.

© 2006-2007 Thinstuff s.r.o

Since all sessions are children of this process, all sessions will be closed if this service is shut down.

3. **The configuration service**. All data used by Thinstuff LX Server are stored in a PostgreSQL database. The access to this database and also some general management tasks are handled by the configuration service. This service can be restarted with out directly affecting any component, but while it is offline operations that require it (e.g. login, session startup/shutdown) might be delayed or fail.
4. **The session**. Each session is a separate X11 server. Thinstuff LX Server automatically takes care of assigning display numbers and security tokens for those servers, and sets the environments of the session programs so that they use this X11 server. Everything that is displayed on this X11 server is transferred to the RDP client, so using remote X11, query mode or other X11 features work as expected.
5. **The PostgreSQL service**. As indicated before, all data are stored in a PostgreSQL database. This database is installed with the Thinstuff LX Server installation directory and will not conflict with any other installed PostgreSQL databases.
6. **The administration interface**. The administration of the Thinstuff LX Server is done via a secure web interface. This interface is served by a lighttpd web server included in the installation. The webserver is running on the https port (443) by default, this can be reconfigured however. To be able to actually log into the web interface and manage anything, at least the PostgreSQL and configuration service have to run.

2 Installation

2.1 Introduction

This manual assumes basic familiarity with the Linux® operating system and your current desktop environment (e.g. GNOME or KDE®). Furthermore you will need to be a privileged user (i.e. root user) to install the package successfully, installation as a normal user is not currently supported. If you do not have the possibility to install the package as a privileged user yourself, please ask your system administrator for assistance.

2.2 Installation layout

The Thinstuff LX Server will be installed into the `/opt/thinstuff/rdpserver` directory. Installation into a different directory is currently not supported. This limitation implies that only a single copy of the server can be installed at any one time. Inside this directory you will find a directory hierarchy similar to your root directory. Apart from very few exceptions, Thinstuff LX Server includes all the

© 2006-2007 Thinstuff s.r.o

system libraries needed to run in its own directory structure, so you will not need to install any additional packages.

If the installer detects a previously installed copy of Thinstuff LX Server, the installer moves it to **`/opt/thinstuff/rdpserver.backup`** before beginning installation. It is possible to keep this directory around so that you can restore the previous installation if you have problems. Previous backups are destroyed when new backups are made.

2.3 Installation steps

As a privileged user, open a console at the location where you downloaded the installation package. It is recommended that you do not stop your currently installed server before upgrading. The installer will automatically stop and (re)start the server during the installation process.

Execute the installation script by typing:

```
bash lxserver-1.2-4108.sh
```

After an introduction screen, the installer will ask you which action you want to perform. Depending on whether you have a previous version installed and which version that is, you get a subset of the following options:

2.3.1 Restore

If you have a backup in **`/opt/thinstuff/rdpserver.backup`** then you can choose to restore it. This stops and deletes the current installation and moves the backup in its place. This will restore the exact state the server was in before the upgrade. Any changes to the configuration made in the meantime are lost.

2.3.2 Install

This will install your copy of Thinstuff LX Server. An existing copy is stopped and backed up as described above. If you already have licenses installed in an existing copy, they will be copied into the new installation automatically. Also a copy of all old configuration files are copied into your new installation with the extension ".old" added to them. Once the installation is complete, the server will be started automatically.

To perform the installation, follow the instruction on the screen. The step about sending system information is completely optional, and this information will be stored completely anonymous. If you chose to send this information, you can review the exact data before it is sent to us.

2.3.3 Upgrade

This option is only available if all of the following conditions are met:

- You already have a Thinstuff LX Server installed in **`/opt/thinstuff/rdpserver`**

- The installed server is at least version 1.1
- The installed server is currently running

This option behaves exactly like "Install" (2.3.2), except that it will keep the changes made in the web interface (profiles, settings, rights), instead of resetting them to their defaults.

2.3.4 Remove

This option will stop and remove any currently installed server.

2.3.5 Exit

This will exit the installer without changing any files.

2.4 First Steps

If you have installed the server for the first time or if you have not been able to perform "Upgrade" (2.3.3) then you should log into the administration web interface now and perform some initial configurations. With your favorite browser, go to https://my.server.url/ (see chapter 8.2 if another application is already running on the https port for this server).

By default only the root user can log into the web interface. Authentication is performed against your system authentication service, so all usernames and passwords will be the same as for a normal login to the system. If you get stuck, please see chapter 3 for more information on using the web interface.

2.4.1 Evaluation Mode

By default the server runs in evaluation mode. This mode is restricted to testing/evaluation purposes and provides a maximum of 5 connections and sessions. Each connection will drop out of the session after 30 minutes and display the login dialog again, after re-login the user can resume the existing sessions for testing purposes.

Please note that the 30 minute restriction is only present in the evaluation mode, if you have any trial version (after registering on our website) or full version all connections will work forever.

2.4.2 Licenses

The first thing you will want to check is the status of your licenses. Navigate to "Cluster Status" -> "License Info" to see if you have any valid licenses installed. If you do not have any valid licenses, then please go to http://www.thinstuff.com/licensing to obtain licenses for your product.

© 2006-2007 Thinstuff s.r.o

2.4.3 Users

All users are eligible to connect to the RDP server, but only the root user can administer it via the web interface by default. If you want to grant other users the right to administer the server, perform the following steps:

- Navigate to "Rights" -> "Users".
- Find the user you want to modify.
- Click the "Rights" link in the rightmost column.
- In the section "User Rights", click the "Edit Rights" link.
- Change the „Login" Right to „Allow".
- Confirm with the "Change Rights" button.

2.4.4 Session Type

By default, the server will start "twm" as a session for the user. You will almost certainly want to change this. To change this, please perform the following steps:

- Navigate to "Settings" -> "Configuration".
- Choose the "default" profile (if the page does not load automatically, hit the "Change Profile" button).
- Activate the "Session" tab (should be activated by default).
- Change the "User application" value. Please note, that the web interface does not detect which desktop environments you actually have installed.
- Optionally change the color depth and maximum resolution of your desktop.
- Confirm with the "Save" button.

You should now have a basic system running. Please see chapters 3 to 6 for more information about the possible methods to configure your server and other issues of day-to-day use.

2.4.5 Starting the server at system startup

We provide a sample init script for Thinstuff LX Server in the file **`/opt/thinstuff/rdpserver/scripts/rdp-server.init.d-template`**. Please see your system documentation on how to install init scripts. The following steps are examples for some systems (they must be performed as root user):

2.4.5.1 LSB compliant systems (most major distributions)

```
cp /opt/thinstuff/rdpserver/scripts/rdp-
server.init.d-template /etc/init.d/rdp-server
```

```
/usr/lib/lsb/install_initd /etc/init.d/rdp-server
```

2.4.5.2 Ubuntu

```
cp /opt/thinstuff/rdpserver/scripts/rdp-
server.init.d-template /etc/init.d/rdp-server

update-rc.d rdp-server defaults
```

2.4.5.3 Gentoo

```
cp /opt/thinstuff/rdpserver/scripts/rdp-
server.init.d-template /etc/init.d/rdp-server

rc-update add rdp-server default
```

2.5 Automating the installation process

It is possible to automate the installation process. The most common case (upgrading the server to a new version) can be handled by executing

```
bash lxserver-1.1.2-3546.sh upgrade! \
   --batch-mode --accept-license
```

from the command line. This will perform the same actions as described in chapter 2.3.3 but without asking any questions. If upgrading is not possible then the "Install" (2.3.2) action is automatically performed.

For more information about the possible options for automated installs, please see the help that comes with the installer:

```
bash lxserver-1.1.2-3546.sh --help
```

2.6 Important files and directories

As noted above, all files are installed in the directory **`/opt/thinstuff/rdpserver`**. The following files and directories are of particular interest:

- **`/opt/thinstuff/rdpserver/scripts/startall.sh`**
  Start the small business server.
- **`/opt/thinstuff/rdpserver/scripts/stopall.sh`**
  Stop the small business server.
- **`/opt/thinstuff/rdpserver/scripts/init.sh`**
  Restart the small business server, this has the same effect as calling **`stopall.sh`** followed by **`startall.sh`**
- **`/opt/thinstuff/rdpserver/licenses/`**
  This directory contains all your current licenses. Licenses must be stored in this directory to work; to install a license simply copy or move it to this

© 2006-2007 Thinstuff s.r.o

location. It is not required to restart the server in order to install or remove licenses.

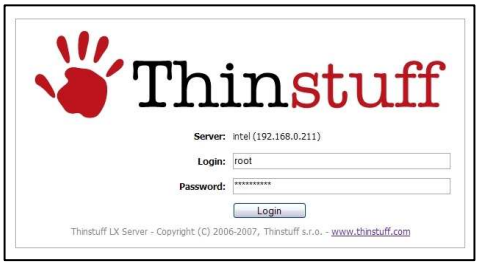
2.7 Making manual backups

Since the Thinstuff LX Server is completely contained in one directory it is very easy to make manual backups of the server. Perform the following steps to backup the current state of your server:

- Call
  `/opt/thinstuff/rdpserver/scripts/cli-adminclient.sh \ --export > /your/backup/file`
  to dump all settings to a file. Backup this file using your favorite backup solution.
- Execute `/opt/thinstuff/rdpserver/scripts/stopall.sh` to stop the Server. This is important, because trying to backup the PostgreSQL database while it is running will most certainly result in a broken backup.
- Backup the `/opt/thinstuff/rdpserver` directory using your favorite backup solution.
- Execute `/opt/thinstuff/rdpserver/scripts/startall.sh` to restart the Server.

© 2006-2007 Thinstuff s.r.o

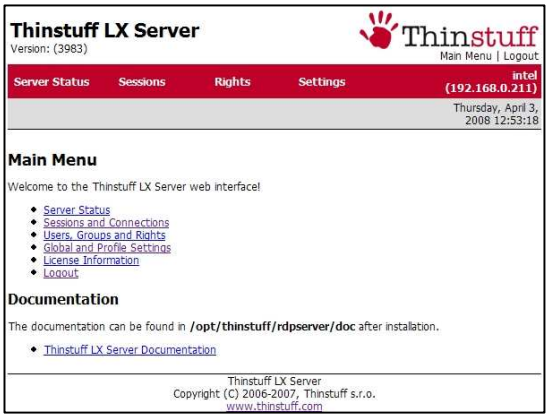
3 Web interface



The Thinstuff LX Server is administered via a web based configuration and management interface. After installing and starting your server, please point your web browser to https://my.server.url/ (Please see section 8.2 if you need to start the web service on a different port, also note that the default setting is the https protocol instead of simple http).

Please log in as root user with your current root password (see section 3.3 on how to configure access for different users). The web interface is split into 4 areas:

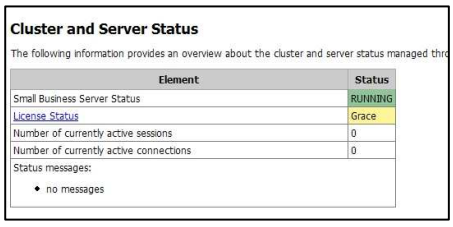
- **Server Status** – Determine current problems quickly.
- **Sessions** – Identify which users are using your services and manage them.
- **Rights** – Configure who has access to the web interface.
- **Settings** – Configure operational parameters for the terminal server and sessions



3.1 Server Status

3.1.1 Server Health

In this section you can get a quick overview of the status of your terminal server. The status is color-coded for easy reference, and eventual problems will show explanatory status messages. There are four different status levels:



- **Running (green)** – Everything is working without problems
- **Warning (yellow)** – The server is working, but one or more components are experiencing problems. It is advised to monitor server behavior to see if the problem is just temporary or to upgrade overloaded resources. Problems could include:
    - CPU, Memory or other resources reach a critical point

- One or more, but not all, copies of a redundant component are reporting errors during operation.

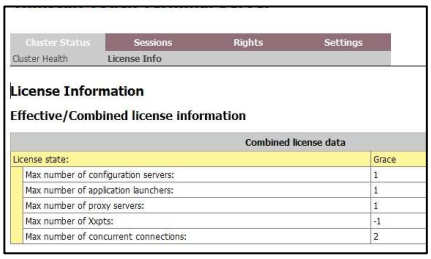
Immediately after a restart of the server, the cluster status may show up yellow, since the components need a few seconds to find acknowledge each other. The status will resolve itself back to green after a short while.

- **Critical (red)** – Similar problems like Warning, but they affect all copies of a redundant component or a non-redundant component. If a server is in status critical then it may still work, but it might fail soon or not work reliable for all connections. It is advised to restart the terminal server as soon as this is conveniently possible, and to upgrade overloaded resources or increase redundancy.
- **Error (red)** – One or more components have definitely failed and the server is not operational anymore. You will need to restart the terminal server.

Additionally this section also shows how many sessions and connection are currently running, as well as precise version information of your server.

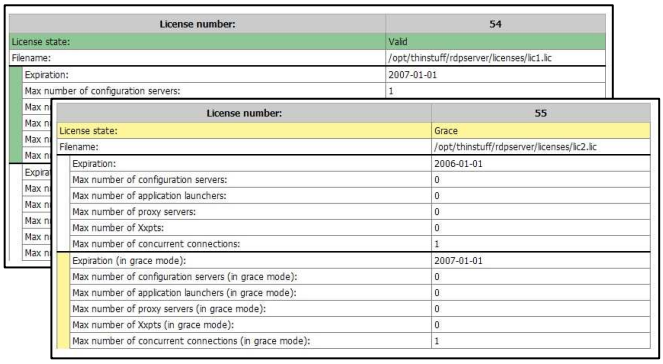
3.1.2 License Info

The second part of the Cluster Status section shows you information about your current licenses. The top part shows a summary, and it will display the effective license values. If some of these values are based on licenses in grace mode (see below) then this section will be marked yellow, otherwise it is marked green.



Below this section you will see information about every license file found in your licenses folder (`/opt/thinstuff/rdpserver/licenses`). Each license can be in one of three states:

- **Valid (green)** – The license is still fully valid
- **Grace (yellow)** – The license is already expired, but is valid a little longer (see the information about when the grace period expires). If a connection to the terminal server is accepted only because of a license in grace period, then the user will be notified of this by a message prior to connecting. Also licenses may have additional restrictions (fewer connections, …) during the grace period.



- **Invalid (red)** – This may have various reasons (invalid hardware id, invalid license file, …).

A valid license will show values for normal operation and for grace operation. The color coding will show which values are in effect currently and when the license will cease to be valid.

3.2 Sessions

Cluster Status
Sessions
Rights
Settings
Sessions
Show all
Refresh
ID Node ID User ID Initial Client Host Profile ID Pid Clients Connected Last Disconnect Time Session Timeout Actions
33 -1 se97031 CADRIMA default 29244 1 -1 Filter Connections Destroy Session
34 -1 authuser CADRIMA login 29293 1 0 Filter Connections Destroy Session
All Connections
ID Proxy Client IP Client Port Session ID Username Resolution Locale Actions
18 30 192.168.0.21 1253 33 se97031 800x600x24 en_US Disconnect
19 30 192.168.0.21 1255 34 not available 800x600x24 en_US Disconnect

This section will list all currently active sessions and connections to the terminal server. Each sessions can have zero, one or more connections. Sessions with zero connections do not currently have users viewing them and will be automatically destroyed after the given session timeout. Sessions with more than one connection are shadowed by one or more users. Internal sessions and connections are marked with a gray background.

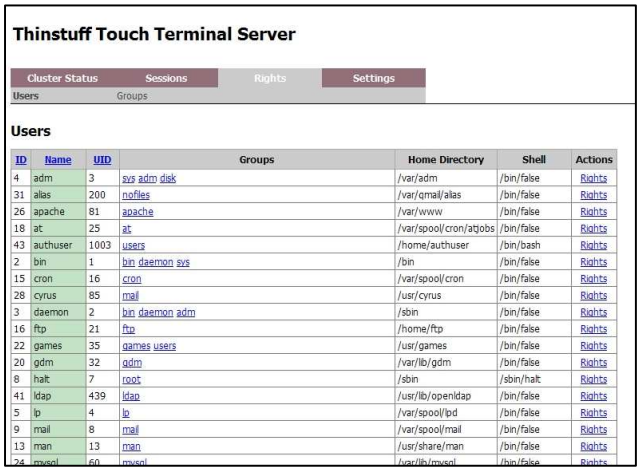
It is possible to destroy a complete session (all connected users will be disconnected) or just a single connection (the session is unaffected, but the timeout may eventually destroy the session if the last connection is removed).

Thinstuff Touch Terminal Server
Cluster Status
Sessions
Rights
Settings
Sessions
Show all
Refresh
ID Node ID User ID Initial Client Host Profile ID Pid Clients Connected Last Disconnect Time Session Timeout Actions
33 -1 se97031 CADRIMA default 29244 1 -1 Filter Connections Destroy Session
Connections for Session 33
ID Proxy Client IP Client Port Session ID Username Resolution Locale Actions
18 30 192.168.0.21 1253 33 se97031 800x600x24 en_US Disconnect

To quickly see which connections are viewing a given session, press the "Filter Connections" button. Only this session, and only connections for this session will be shown until the "Show all" button is pressed.

3.3 Rights

The website and the terminal server use system users and passwords for authentication. Not every user has access to the web interface though. The access to the web interface and the rights to view/modify different settings can be configured per user. After the installation the root user has full access (all rights) and no other user has any rights.

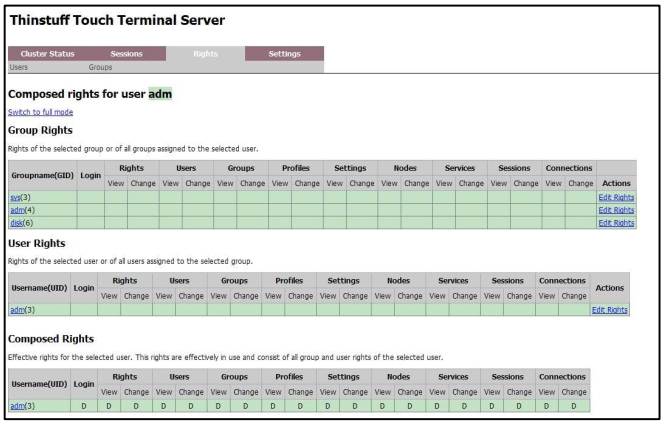

Thinstuff Touch Terminal Server
Cluster Status
Sessions
Rights
Settings
Users
Groups
Users
ID Name UID Groups Home Directory Shell Actions
4 adm 3 sys adm disk /var/adm /bin/false Rights
31 alias 200 nofiles /var/qmail/alias /bin/false Rights
26 apache 81 apache /var/www /bin/false Rights
18 at 25 at /var/spool/cron/atjobs /bin/false Rights
43 authuser 1003 users /home/authuser /bin/bash Rights
2 bin 1 bin daemon sys /bin /bin/false Rights
15 cron 16 cron /var/spool/cron /bin/false Rights
28 cyrus 85 mail /usr/cyrus /bin/false Rights
3 daemon 2 bin daemon adm /sbin /bin/false Rights
16 ftp 21 ftp /home/ftp /bin/false Rights
22 games 35 games users /usr/games /bin/false Rights
20 gdm 32 gdm /var/lib/gdm /bin/false Rights
8 halt 7 root /sbin /sbin/halt Rights
41 ldap 439 ldap /usr/lib/openldap /bin/false Rights
5 lp 4 lp /var/spool/lpd /bin/false Rights
9 mail 8 mail /var/spool/mail /bin/false Rights
13 man 13 man /usr/share/man /bin/false Rights

© 2006-2007 Thinstuff s.r.o

3.3.1 Users

This section shows all the known users in the system. This list is synchronized with the system every few seconds, so if you add new system users they should show up here a few seconds later. For every user the list of groups this user is a member of is also shown. Click a group to see all the users in this group. Click on the Rights link to view the rights assigned to this user.

In this view you can see which rights are set for the groups the user is member of, for the user itself, and what effective rights this results in. Right composition follows the following rules (in this order):



1. User rights override group rights. If a right is set for a user this is used, otherwise the group rights are used.
2. Group rights are merged. It is sufficient to have "Allow"/"Deny" set in one of the groups a user is member of.
3. "Deny" overrides "Allow":
    a. If a user has "Allow" set, but inherits "Deny" from group rights, then the final right is "Deny".
    b. If the groups a user is member of have both "Allow" and "Deny" set then the group right is "Deny".
4. If rules 1 to 3 do not produce any result (nothing set) then the resulting right is "Deny".

There are currently 20 rights:

- **Login** – This user is allowed to log on to the web interface.
- **Join All Sessions** – This user is allowed to join (shadow) sessions of all users. If this is not set, a user can only join (shadow) sessions he created himself. See chapter 6 for more information about shadowing.
- **View/Change Rights** – View or change the assignment of rights. With this and all the other rights which have a "View" and "Change" representation, the "View" version gives read-only access, while the "Change" version allows modification. Typically "View" is a prerequisite for "Change" since the user interface needs to display the values before you can change them.
- **View/Change Users** – View or change the list of system users.
- **View/Change Groups** – View or change the list of system groups.

© 2006-2007 Thinstuff s.r.o

- **View/Change Profiles** – View or change the profiles (see chapter 3.4) the terminal server uses.
- **View/Change Settings** – View or change the settings (see chapter 3.4) the terminal server uses.
- **View/Change Nodes** – This is only for clustered servers, it is not currently in use.
- **View/Change Services** – This is only for clustered servers, it is not currently in use.
- **View/Change Sessions** – View or change (destroy) sessions (see chapter 0).
- **View/Change Connections** – View or change (destroy) connections (see chapter 0).

Note, that some of these rights are prerequisites for other rights. For example it is necessary to have at least read-only access to the user list to be able to view or change user rights.

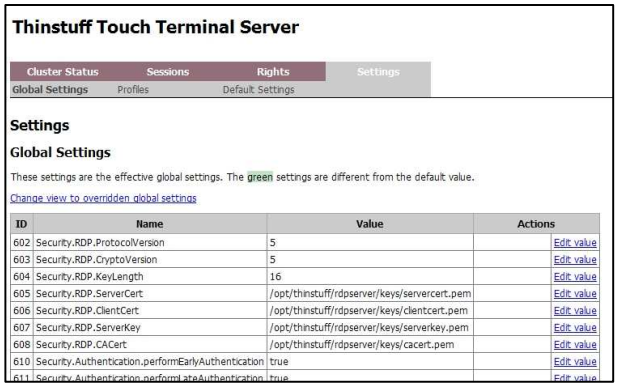
Groups
Total number of grous: 65. Showing results 1 to 20.
ID Name GID Users Actions
2 adm 4 3 users Rights
3 apache 81 1 users Rights
4 at 25 1 users Rights
5 audio 18 1 users Rights
6 authuser 441 no users Rights
7 bin 1 3 users Rights
8 cdrom 19 1 users Rights
9 cdrw 80 1 users Rights
10 console 17 no users Rights
11 cron 16 1 users Rights
12 crontab 445 no users Rights
13 daemon 2 3 users Rights
14 dialout 20 1 users Rights
15 disk 6 3 users Rights
16 floppy 11 2 users Rights
17 ftp 21 1 users Rights
18 games 35 1 users Rights
19 gdm 32 1 users Rights
20 haldaemon 447 1 users Rights
21 kmem 9 no users Rights
Showing all groups: Filter groups with GID < 1000 and not root.
Page 1 2 3 4

3.3.2 Groups

Same as the user list, this shows all the known groups in the system. This list is also synchronized with the system every few seconds. Click on a the users link of a group to show all users for this group. Click the rights link to change the rights for this group (analogous to the user rights dialog).

3.4 Settings

Settings govern different aspects of the Thinstuff LX Server behavior. These range from port allocation to various CPU or bandwidth optimizations. There are two different kinds of settings:


Thinstuff Touch Terminal Server
Cluster Status Sessions Rights Settings
Global Settings Profiles Default Settings
Settings
Global Settings
These settings are the effective global settings. The green settings are different from the default value.
Change view to overridden global settings
ID Name Value Actions
602 Security.RDP.ProtocolVersion 5 Edit value
603 Security.RDP.CryptoVersion 5 Edit value
604 Security.RDP.KeyLength 16 Edit value
605 Security.RDP.ServerCert /opt/thinstuff/rdpserver/keys/servercert.pem Edit value
606 Security.RDP.ClientCert /opt/thinstuff/rdpserver/keys/clientcert.pem Edit value
607 Security.RDP.ServerKey /opt/thinstuff/rdpserver/keys/serverkey.pem Edit value
608 Security.RDP.CACert /opt/thinstuff/rdpserver/keys/cacert.pem Edit value
610 Security.Authentication.performEarlyAuthentication true Edit value

- **Global Settings** – They are always valid, and are independent of individual sessions or connections. They include things like the port the RDP server listens on for connections.
- **Profile Settings** – These are only valid for a given session or connection. Each session and connection is run under a specific profile, and different profiles can have different values for those settings.

The number of settings you can see on each of the settings pages depends on your view level. Three levels enable options based on their complexity:

- Level 0 (Standard) – This contains only the most often used settings. It will be sufficient for most tasks but may not allow more complex setups.
- Level 1 (Advanced) – This contains all settings of level 0 and additionally settings which control more complicated behavior of the server. You will likely have to change a few of those parameters, but typically not on a day-to-day basis.
- Level 2 (Expert) – This contains all settings. You will usually not use this level. Some of the settings are not safe to change without risking the stability of your server, so be careful when setting these. Never change those unless you have good reason to do so, and have read the help for the settings you are about to change.

3.4.1 Global Settings

Global settings are settings which are needed during server startup or at other times when a matching into profiles is not possible. To get an explanation of the settings, move your mouse over the setting name, and a popup window will show you help information. Additionally the information will be displayed when you edit a value.

There are two possible display modes for this page. By default the effective settings will be shown. This means that all settings are displayed with their current value. If the current value is not the default value, then it is marked in green.

By switching to the "overridden values" view, only those values are displayed for which the value is not the default value, all the other settings are not displayed at all. To add a new setting (for editing), use the drop-down box.

3.4.2 Profiles

It is often necessary to change settings based on which user is connecting to the server, where this user is coming from or which hardware this user has. To allow this, the terminal server has the concept of profiles. Each profile stores a set of setting values, and whenever a client connects to the server, a profile is selected. The number of profiles you need depends on your specific case, but in general you will create one profile for each group of users who need a different kind of setup.

The selection of the profile for a connection is based on the "Match" settings in the profiles. There are three different criteria which can be used for matching:

- **user** – Match only if the user is one of the specified list.
- **group** – Match only if the user is a member of the specified groups.

© 2006-2007 Thinstuff s.r.o

- **host** – Match only if the host the user connects from is in the specified list.

Each of the criteria is specified by two settings. One enables the criteria, the other specifies the values to match against. The following examples demonstrate this behavior:

```
Example 1: This profile will match all users in the
"sales" group

Match.users.enable=false
Match.groups.enable=true
Match.groups.values=[sales]
Match.hosts.enable=false
```

```
Example 2: This profile will match all users logging
in from the hosts "lobby" and "infopoint"

Match.users.enable=false
Match.groups.enable=false
Match.hosts.enable=true
Match.hosts.values=[lobby infopoint]
```

```
Example 3: This profile will match if the user root
is connecting from the "lobby" machine

Match.users.enable=true
Match.users.values=[root]
Match.groups.enable=false
Match.hosts.enable=true
Match.hosts.values=[lobby]
```

As you can see, examples can create a conflicting situation. Consider what happens if a user from the "sales" group logs in from the host "lobby". Both examples one and two will match, but only one profile can be active; which will get chosen? The answer is that example one will be the profile for this connection. This is because example one is a more "specific" match than example two. The rules for this rating are as follows:

- If a match is based on a small group of possible values this is more specific than matching a large group of values (matching a profile that only allows 2 users if more specific than matching one that allows 10).
- Matching a profile with multiple criteria is more specific that matching a profile with just a single criteria.
- In case of ties, the following list determines the winner:

© 2006-2007 Thinstuff s.r.o

- The match is based on the username.
- The match is based on the main group of a user.
- The match is based on the other groups of a user.
- The match is based on the hostname.

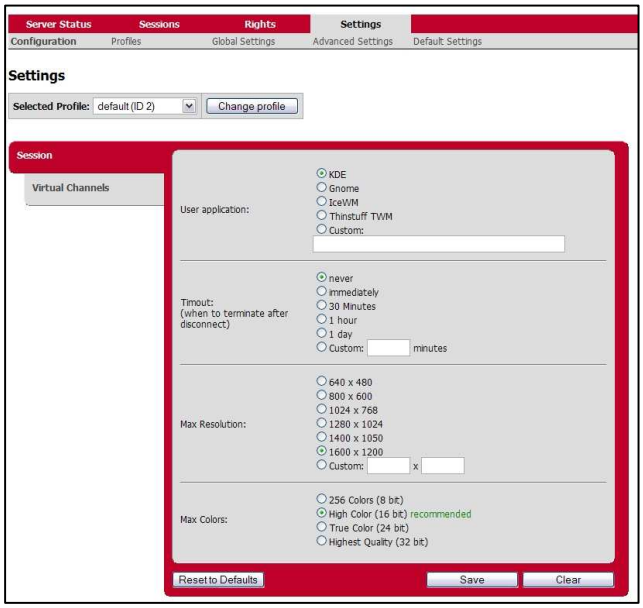
Please note, that enabling a criteria but leaving the value list empty will make it impossible to ever match this profile. If you want to ignore a criterion, disable it.

Additionally you can also set a profile to "passive". This makes it impossible to match this profile, no matter what the criteria are set to. This is used for example for the special "login" profile. During the authentication process, all users are always temporarily using this profile, but you do not want anyone to use it for the actual session.

Once the profile is selected, the settings in this profile apply for that client. There exist two exceptions to this rule:

- During login, a user will always be in the special "login" profile.
- If a user connects to an already existing session (by reconnect or by shadowing), then he will use the profile the session had when it was first created.

3.4.3 Settings Wizard



Using the settings wizard, you can change the most common settings in an easy way.

Use the drop-down box on top to select which profile you want to work on. If your browser does not support Javascript, then you will have to use the "Change Profile" button to commit your change.

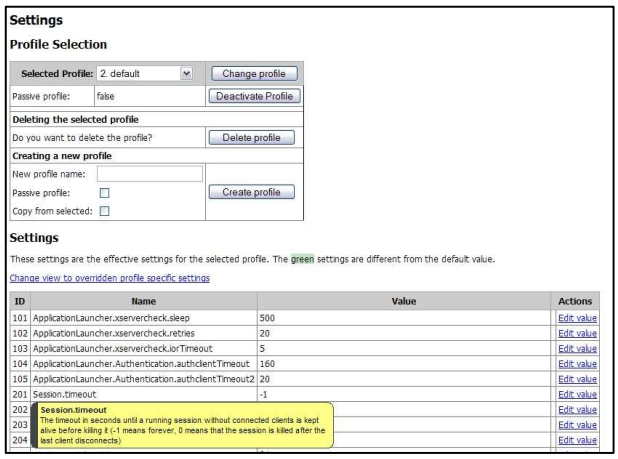
Select one of the available tabs. Depending on the type of profile, there will be different tabs available. In the area to the right you, change the values as you need. Commit your changes with the Save button, or undo them with the Cancel button. Using the "Restore to Defaults" button, you can reset the whole tab to factory default values.

3.4.4 Advanced Settings

In this section you can change profile settings as well as manage the profiles themselves.

© 2006-2007 Thinstuff s.r.o

Use the drop-down box on top to select which profile you want to work on. If your browser does not support Javascript, then you will have to use the "Change Profile" button to commit your change. The block below the profile selection allows you to perform basic operations on the profile, like activating, deleting or copying it.


Settings
Profile Selection
Selected Profile: 2. default
Change profile
Passive profile: false
Deactivate Profile
Deleting the selected profile
Do you want to delete the profile?
Delete profile
Creating a new profile
New profile name:
Passive profile:
Copy from selected:
Create profile
Settings
These settings are the effective settings for the selected profile. The green settings are different from the default value.
Change view to overridden profile specific settings
ID
Name
Value
Actions
101 ApplicationLauncher.xservercheck.sleep 500 Edit value
102 ApplicationLauncher.xservercheck.retries 20 Edit value
103 ApplicationLauncher.xservercheck.iorTimeout 5 Edit value
104 ApplicationLauncher.Authentication.authclientTimeout 160 Edit value
105 ApplicationLauncher.Authentication.authclientTimeout2 20 Edit value
201 Session.timeout -1 Edit value
202 Edit value
203 Edit value
204 Edit value
Session.timeout
The timeout in seconds until a running session without connected clients is kept alive before killing it (-1 means forever, 0 means that the session is killed after the last client disconnects)

Below is a list of the settings you can change for this profile. This part works exactly like the Global Settings page (3.4.1).

Once a session is created with a specific profile, the settings of this profile are copied into the session. This means that modifying the profile after a session has been created will not affect the session.

A description of all settings can be found in Appendix A – Settings Descriptions. Here is a selection of the most important ones:

3.4.4.1 Applications.session.command

This setting specifies the command that is started as the session for a user in this profile. You will almost always want to change this (default is a version of "twm" included in Thinstuff LX Server), and typically you will set this to a command that starts up a desktop environment. The command will be searched for in the users path, so you do not need to specify a full path. The session of a user is closed as soon as this command exits, so if you use a shell script, you have to make sure the main program is not started in the background. Please see the documentation for your desktop environment on how to start it. Here are a few short samples:

- For KDE, type **`startkde`**.
- For Gnome, type **`gnome-session`**.
- For IceWM, type **`icewm-session`**.

You can specify additional command line parameters with the setting **`Applications.session.params`** and give an initial working directory for the application with **`Applications.session.workingdir`**.

There exists two special value for this setting. If the setting starts with "-query", then it is not taken as an executable, but instead will perform an XDMCP query call to the host given after the "-query". For example "-query cadServer" will try to open an XDMCP query session on the server "cadServer".

© 2006-2007 Thinstuff s.r.o

If the value of this setting is empty, then no program will be started for the session. The session will end, once the virtual X11 server terminates. This can be used if you want to start programs into the server manually (eg: from an external process).

3.4.4.2 Session.timeout

When the last user disconnects from a session, the session is not automatically closed. Instead all programs continue to run, and it is possible to reconnect later. This timeout specifies the maximum amount of time in seconds, such a disconnected session is allowed to exist. If no user reconnects by this time, it is automatically closed. The default value of -1 means never to close this session, a value of 0 means the session is destroyed immediately after a disconnect.

3.4.4.3 Session.maxWidth

Together with Session.maxHeight and Session.maxDepth, these specify the maximum allowed screen resolution and bit depth. Clients can use lower values when connecting, but not higher. If a client tries to connect with a higher resolution, he will get the set maximum resolution.

Each session has to allocate memory for the highest allowed resolution. This means that limiting the resolution to lower values means less memory usage per session. So if you know that your clients have limited screens (eg: a PDA), then using smaller values here will result in less memory usage. Here are some sample memory values for typical resolutions (each given for 8, 16 and 24bit color depth):

- 640x480: 1/2/4MB per session
- 1024x768: 2.5/5/10MB per session
- 1600x1200: 6/12/23MB per session

Please note that 24bit color depth not only uses more memory, but also increases the CPU usage on the server compared to 8 or 16 bit color depths. We recommend using 16 bit color depths as a best compromise between performance and image quality.

3.4.4.4 RdpServer.verifyDisconnect

This setting controls whether connections immediately close when the user tries to close the RDP client, or if the client should first display the dialog that informs the user that it is possible to reconnect to this session later if he does not log out. Currently this feature is not supported by rdesktop.

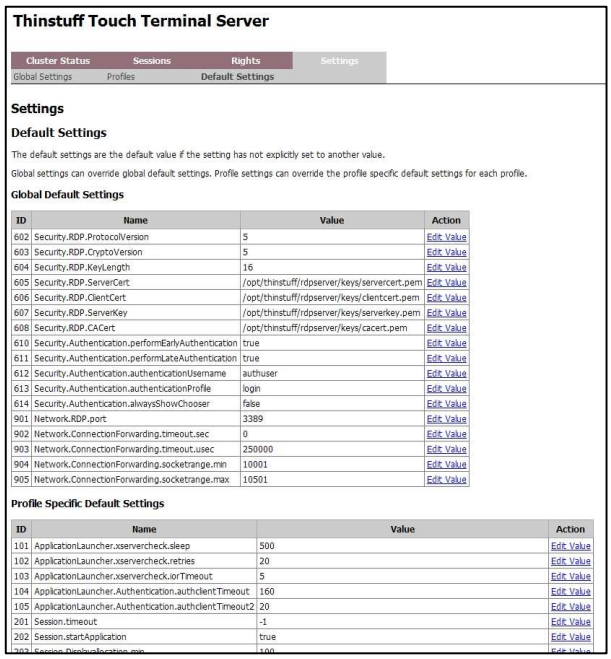
3.4.5 Default Settings

In this section you can view and change the system defaults for settings. It is not recommended that you actually change system defaults since there is no convenient way to reset them back to factory defaults.

© 2006-2007 Thinstuff s.r.o

4 Session startup

This chapter explains in more detail how sessions are started, and what possibilities you have to fine-tune this behavior.


Thinstuff Touch Terminal Server
Cluster Status
Sessions
Rights
Settings
Global Settings
Profiles
Default Settings
Settings
Default Settings
The default settings are the default value if the setting has not explicitly set to another value.
Global settings can override global default settings. Profile settings can override the profile specific default settings for each profile.
Global Default Settings
ID Name Value Action
602 Security.RDP.ProtocolVersion 5 Edit Value
603 Security.RDP.CryptoVersion 5 Edit Value
604 Security.RDP.KeyLength 16 Edit Value
605 Security.RDP.ServerCert /opt/thinstuff/rdpserver/keys/servercert.pem Edit Value
606 Security.RDP.ClientCert /opt/thinstuff/rdpserver/keys/clientcert.pem Edit Value
607 Security.RDP.ServerKey /opt/thinstuff/rdpserver/keys/serverkey.pem Edit Value
608 Security.RDP.CACert /opt/thinstuff/rdpserver/keys/cacert.pem Edit Value
610 Security.Authentication.performEarlyAuthentication true Edit Value
611 Security.Authentication.performLateAuthentication true Edit Value
612 Security.Authentication.authenticationUsername authuser Edit Value
613 Security.Authentication.authenticationProfile login Edit Value
614 Security.Authentication.alwaysShowChooser false Edit Value
901 Network.RDP.port 3389 Edit Value
902 Network.ConnectionForwarding.timeout.sec 0 Edit Value
903 Network.ConnectionForwarding.timeout.usec 250000 Edit Value
904 Network.ConnectionForwarding.socketrange.min 10001 Edit Value
905 Network.ConnectionForwarding.socketrange.max 10501 Edit Value
Profile Specific Default Settings
ID Name Value Action
101 ApplicationLauncher.xservercheck.sleep 500 Edit Value
102 ApplicationLauncher.xservercheck.retries 20 Edit Value
103 ApplicationLauncher.xservercheck.iorTimeout 5 Edit Value
104 ApplicationLauncher.Authentication.authclientTimeout 160 Edit Value
105 ApplicationLauncher.Authentication.authclientTimeout2 20 Edit Value
201 Session.timeout -1 Edit Value
202 Session.startApplication true Edit Value

4.1 Connection setup and authentication

The client connects to the Thinstuff LX Server through the proxy service. This service will set up a new connection on the server and initiate the authentication process. If the credentials given by the client initially (prefilled username/password) are enough to authenticate the user, then the server immediately continues with the session setup. The global setting "Security.Authentication.performEarlyAuthentication" can be used to disallow the authentication on prefilled usernames/passwords. In this case the following steps will always be performed.

Otherwise a temporary session under the authentication profile is created and a username and password dialog is shown. Once the user is authenticated, the server continues with session setup. Similar to above, the global setting "Security.Authentication.performLateAuthentication" can be used to disable the usage of this authentication session. If this is set to "false", then a user must provide a prefilled username/password or the authentication will fail.

The following settings also modify the behavior of these steps:

- Network.RDP.port: TCP port the proxy listens on. The default RDP port is 3389
- Security.Authentication.PAM-Service: The name of the pam service to be used. The configuration of this service is in the corresponding file in **`/etc/pam.d`**. See chapter 10 for some samples.
- Security.Authentication.caseSensitive: If your authentication service is not case sensitive, set this to false. Note: this only changes name lookups internal to Thinstuff LX Server, it will not change the way your authentication service actually works.
- Security.Authentication.authenticationUsername: The system user under which the login session (if needed) is started. The default (authuser) is automatically created by the installation process of Thinstuff LX Server.

© 2006-2007 Thinstuff s.r.o

- Security.Authentication.authenticationProfile: The profile used for login sessions.

4.2 Session setup

The first step in session setup is to find existing sessions the user can connect to. Three scenarios exist:

- No sessions available: In this case the server creates a new session
- One session available: The server connects the user to this session automatically
- More sessions available: The server shows a chooser dialog (if necessary, a login session is created to show the dialog in) to ask the user which session she wants to connect to.

By default a session is "available" if it was created by this user, and is not currently connected to by anyone. There are a few settings you can use to modify this behavior. These settings are profile settings, meaning that they only apply to sessions created under their profile.

- Session.matchPerUser: If false then ignore the username. Users can connect to sessions made by any user under this profile (this is a potential security risk).
- Session.matchPerClienthost: If true, then use the hostname in matching. This means that a user will only see sessions created by himself and created from the same client machine.
- Session.reconnectToConnected: If true, consider sessions that already have connections to be available. This will usually result in a single user not being able to create more than one session (since the second client he starts will automatically join the first session).

If no suitable session was found, the server will start a new session for the user. This involves the following steps:

- A new virtual X11 server is started as user root (the binary is called Xxpt).
- All of the following steps will be performed under the privileges of the user for whom the session is created.
- An X11 authentication cookie is automatically created for the user.
- The server sets up the keyboard layout for the session by calling **`/opt/thinstuff/rdpserver/scripts/updatexkb.sh`**. This file is potentially called multiple times with variations of the locale until a working one is found. You can modify this file to perform special handling of the locales. See chapter 5 for more information about locales.
- The server sets the following environment variables for the session:

© 2006-2007 Thinstuff s.r.o

- THINSTUFF_TOUCH_SESSION_ID: unique identifier of the session. You can use this to identify the session in the web interface (see chapter 3.2)
- THINSTUFF_TOUCH_SESSION_CLIENT_NAME: hostname the client sent to the server. This is not necessarily the true hostname of the client.
- THINSTUFF_TOUCH_SESSION_CLIENT_IP: IP address of the client. This is the IP address of the connection we received. If the connection is routed via proxies or firewalls, this may not be the true IP address of the client.
- THINSTUFF_TOUCH_SESSION_PROFILE_ID: unique identifier of the profile this session uses.

Since it is not possible to modify environment variables once a process is already running, the environment may become invalid if the client has disconnected and reconnected in the meantime. Thus the client IP address and name will always be those of the client who originally created the session.

- If the "Session.sessionFiles" setting is not empty, then the server will call the script **`/opt/thinstuff/rdpserver/scripts/sessionFile.sh`** with its value as parameter. By default this script copies the value of the aforementioned environment variables into a file in this directory. This file can be used in cases where the environment variables are not available (eg: the session runs on a different server with a remote X11 connection).

  For reasons of consistency, the same limitations as for the environment variables apply in cases where the client disconnects and reconnects.
- The session program (if available) is started. If the session program is set to "-query …" or empty then this step is skipped.
- If this session is a login session, then the authentication program is started automatically to display a prompt for username and password.

5 Internationalization and Localization

In a terminal server environment special considerations must be taken into account when it comes to internationalization and localization. Mostly this is the case because the client is running on a different computer, whose locale settings are not necessarily the same as the server. In addition it is possible that a user switches between different client machines with different locales.

The RDP client sends the locale of the client system to the server. This includes the language setting, as well as the keyboard layout. Thinstuff LX Server can use this information to set the locale and keyboard layout of the sessions accordingly. This is split into two different parts:

© 2006-2007 Thinstuff s.r.o

5.1 Language

Setting the language will give the programs on the server the possibility to display dialogs and error messages in the native language of the user. This does not change the keyboard layout or allow the user to enter text in the local language. Two different settings are available to change this behavior:

- Session.ctypeFromKeyboard: This setting will allow basic processes to be locale aware. This includes correct capitalization, sort order and similar things. Because of the way X11 works, this also affects how dead keys are composed. This means that disabling this might break some details of keyboard layouts.
- Session.languageFromKeyboard: This setting will allow programs to display themselves in the native language.

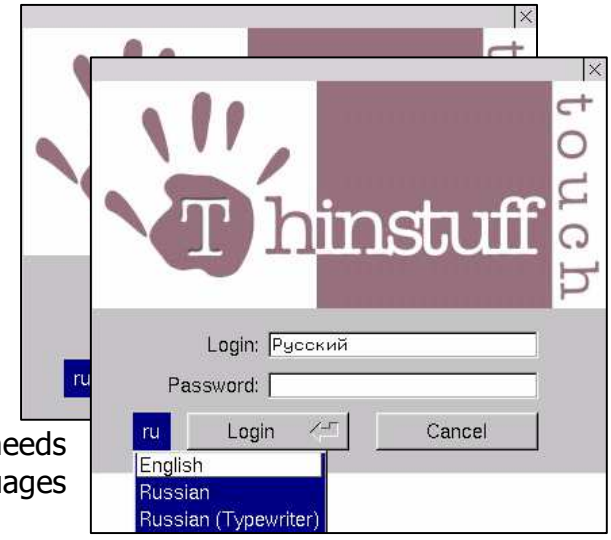
5.2 Keyboard Layout

Setting the keyboard layout correctly allows users to enter characters in their native language. Use "Session.changeKeyboard" to disable this feature.

5.3 Caveats

The first thing to consider is the topic of usernames and passwords and native language characters. By default Linux usernames and passwords can only contain a very limited set of characters, so it might not be possible to enter usernames and passwords with a native keyboard layout. To work around this problem, the login window displays a blue button with the current keyboard layout in the lower left corner. Clicking this button will show a menu where you can select between different keyboard layouts. The items in this menu are generated automatically as follows:

- A standard U.S. English (QWERTY) keyboard layout
- All available keyboard layout variants for your current client locale.



By default, this button only controls the keyboard layout inside the login session, since the main purpose is to allow input of English usernames on regional keyboards. But, if you set "Session.keepLanguageFromLogin" to "true", then the keyboard layout last selected in the login screen will be used to start the session, instead of the language the client has sent on connection.

The second issue that needs consideration is the handling of languages

and keyboard layouts by your desktop environment. Many environments bring their own tools, often in the form of small applets that run in the system tray, which can be used to switch languages or keyboard layouts. In the usual case, those tools will try and restore the settings that were used when this user logged off the last time. Since our server already sets up the keyboard layout, this is not only unnecessary, but can potentially undo the changes we already made. We recommend that you do not use such tools, and that you disable the keyboard layout handling of your desktop environment altogether.

Gnome may exhibit error messages regarding keyboard layouts. If your system shows such warnings, please perform the following steps inside your Gnome session:

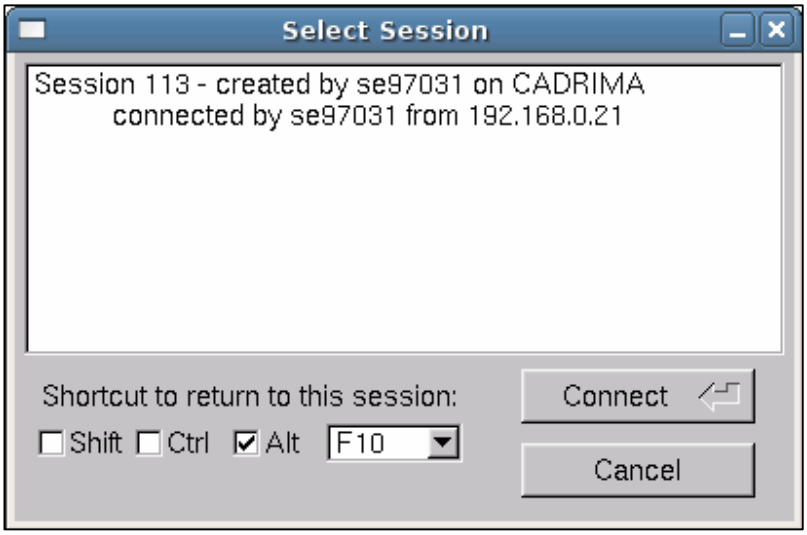
- go to "Desktop" -> "Preferences" ->"Keyboard"
- open the "Layouts" tab
- click the "Reset to Defaults" button.

6 Joining sessions (shadowing)

As outlined in chapter 1.1.5, Thinstuff LX Server provides extensive shadowing capabilities. The process of joining sessions is handled by **`/opt/thinstuff/rdpserver/bin/thinstuff_touch_authenticationclient`**. This program should be in the search path of the current user, so just typing "thinstuff_touch_authenticationclient" in the console or a desktop shortcut should be enough to start it.

Upon starting, it displays a list of sessions which are eligible to join for this user, similar to the one used when connecting to the server. Depending on the "Join All Sessions" right (3.3.1) these are either all the sessions on the server, or just those belonging to the current user.

It is possible to return to the session the shadowing was initiated form, by using a special key combination. By default this key combination is ALT+F10. The dialog used to select a session for joining has controls in the lower left corner for choosing a different key combination.



If more than one user are viewing the same session, some special cases need to be taken into the consideration. The first is the issue of user privileges. When joining a session, you automatically assume the identity of the user for whom this session was started. This not only applies to programs started, but also to operations with Thinstuff LX Server, like joining yet another session.

The second issue is that each operation performed in a session is of course seen by every connection in that session. Also, the server can not distinguish who actually started a program, so if more than one connection exist for a session, and one of them joins yet another session, then all of the connections in this session will join the new session.

7 Virtual Channels

RDP is capable of transmitting extra information, besides the visual content of your desktop. LX Server 1.2 is capable of synchronizing the server clipboard with the client clipboard and also of sending sound from the server to the client. To use these features, your client has to support them. Most RDP clients do, however some (e.g. rdesktop) might need some extra settings to enable them.

By default both clipboard and remote sound are enabled. You can disable them, or change the parameters using the configuration wizard.

To use sound, your applications need to support either ESD or pulse-audio. Support and/or plugins are available for most programs and desktop environments. Please see your applications manual on how to enable ESD/pulse-audio sound. If your server does not have any sound cards built in, then most programs should work out-of-the-box using auto-detection of sound output.

8 Advanced configuration

Some configurations are not possible via the web based configuration and management interface. These include the configuration of basic services, like the webserver or the database server which are needed by the web interface to work properly.

8.1 Database configuration

The default database configuration accepts incoming connections only through UNIX sockets stored in `/opt/thinstuff/rdpserver/var/lib/postgres`. The default user for the integrated postgres daemon is "thinpost". This should prevent any naming and user conflicts with existing PostgreSQL installations.

8.2 Web server configuration

The terminal server uses lighttpd (http://www.lighttpd.net/) as web-server component. It can be configured with the included and documented lighttpd configuration file which can be found at:

```
/opt/thinstuff/rdpserver/etc/lighttpd/lighttpd.conf
```

If you need to change the port the web server listens on, change the value "server.port" to your desired port (default is 443 for https operation). If you want to disable https, then please chance "ssl.engine" to "disable". Note that in that case you also should change the web port to 80, this does not happen automatically.

For more information about lighttpd configuration, please see http://trac.lighttpd.net/trac/wiki.

Reference of the most important settings:

- **server.port** – change the port of the web server (default: 443/https), this is especially necessary if another web server using port 443 is running on the same host as the terminal server.
- **server.bind** – change the address the web server is bound to (default: any interface).
- **ssl.engine** – enable or disable the SSL mode (default: enable).
- **ssl.pemfile** – the PEM file which contains the server SSL private key and client certificate (change this to your SSL certificate to use it instead of the default self-signed certificate).

8.3 Command-line client

The command line client is the second management client next to the web interface and can be used to perform the following tasks:

- get and set global, default and profile settings
- manage profiles
- get a list of users and groups
- manage user and group rights
- query server status information

8.3.1 Return codes and command input/output

The command line client reads commands from the command line, standard input or a file. The default is to read from standard input in interactive mode (if no parameters are given).

Command results are printed to standard output (stdout), error messages and everything else to standard error (stderr).

On success the client returns with exit code 0.

© 2006-2007 Thinstuff s.r.o

8.3.2 Starting the command line client

To start the command line client please execute the file **`/opt/thinstuff/rdpserver/scripts/cli-adminclient.sh`** or go to the scripts directory and simply call **`./cli-adminclient.sh`**.

Interactive mode:

```
#./cli-adminclient.sh
```

Passing a command in the command line:

```
#./cli-adminclient.sh [command]
```

Passing commands to the client standard input:

```
# cat commandfile > ./cli-adminclient.sh
```

Reading a file with commands:

```
# ./cli-adminclient.sh --inputfile commandfile
```

By default the client connects to a server running at localhost and tries to login with the username of the calling user. Please see the command line options on how to connect to remote servers or login with another user.

8.3.3 Command line options

Following options are available:

Option	Description
--help	show a short help message
--longhelp	show a long help message
-u, --user	server username (default: USER environment variable or root if not present)
-h, --host	server hostname (default: localhost)
-p, --port	server port (default: 2911)
--inputfile	a file to read commands from (optional)
--export	export the state (settings,…) of the server (this is a separate mode not accepting any commands)
--poll	poll the server if the XMLRPC interface is up, returns 0 on success, 1 on error (this is a separate mode not accepting any commands)

© 2006-2007 Thinstuff s.r.o

8.3.4 Datasets

Commands are actions on virtual datasets such as settings, server status and users. Such actions can query data or set data.

Example (output with stderr redirected to /dev/null):

```
# ./cli-adminclient.sh get version
3003
1.1
Thinstuff LX Server
Tue Jan 30 17:05:46 CET 2007
```

This example queries the server version, which consists of: build number, version, product name and build date. The action performed was "get".

Each dataset has a different set of actions to be executed and features to be set and queried. The following list shows all available datasets and their actions (the commands are shown without the invocation of cli-adminclient.sh):

8.3.4.1 Dataset: users

Get a list of all users:

```
# get users
```

Get a specific detail (id, uid, name, homedir, shell) of a user selected by id or name (<id> is a placeholder for the id to select and <name> for the name to select):

```
# get (id|uid|name|homedir|shell) of users
(id:<id>|name:<name>)
```

Example:

```
# get uid of users name:root
0
```

8.3.4.2 Dataset: groups

Get a list of all groups:

```
# get groups
```

Get a specific detail (id, gid, name) of a group selected by id or name (<id> is a placeholder for the id to select and <name> for the name to select):

```
# get (id|gid|name) of users (id:<id>|name:<name)
```

Example:

```
# get name of groups id:0
```

© 2006-2007 Thinstuff s.r.o

```
root
```

8.3.4.3 Dataset: version

Get full version information:

```
# get version
```

Query specific version parts (revision,version,product,builddate):

```
# get (revision|version|product|builddate) of
version
```

Example:

```
# get revision of version
3003
```

8.3.4.4 Dataset: clusterhealth

Get all cluster/server health information

```
# get clusterhealth
```

Get specific cluster/server health information

```
# get
(currentsessions|currentconnections|totalfreememory)
of clusterhealth
# get (health|healthtext|errors) of clusterhealth
```

Example (get the number of currently running sessions, return value is 8 sessions):

```
# get currentsessions of clusterhealth
8
```

8.3.4.5 Dataset: sessions

Get all sessions:

```
# get sessions
27 2 16859 4 0 never lap1 1
```

Returns a list of all sessions providing the following information (in order):

- session ID
- user ID
- session PID
- profile ID

© 2006-2007 Thinstuff s.r.o

- session timeout
- time of last client disconnect
- hostname of the client which created the session
- number of connections to this session

8.3.4.6 Dataset: connections

Get all connections:

```
# get connections
```

Get all connections of a specific session (in this example query all connections of session 27):

```
# get connections sessionid:27
5 27 800x600x8 127.0.0.1:46251 11 en_US 25
```

The result is a list of connections with the following information in each line:

- connection ID
- session ID
- current width x height x bits per pixel
- RDP client address and port
- User id (internal id), this value is -1 for connections where the user is unknown (e.g. during login)
- Locale (e.g. en_US, de_DE)
- Proxy handling this connection

8.3.4.7 Dataset: settings.global

Get a list of all global settings:

```
# get settings.global
```

Query a specific feature of a setting:

```
# get (id|name|type|isset|islist) <name> of
settings.global
# get (level|value|defaultvalue) <name> of
settings.global
```

Example:

```
# get value Network.RDP.port of settings.global
3389
```

Set a value of a global setting:

```
# set value Network.RDP.port of settings.global to
3389
```

8.3.4.8 Dataset: settings.default

Get a list of all default settings:

```
# get settings.default
```

Query a specific feature of a setting:

```
# get (id|name|type|islist) <name> of
settings.default

# get (level|value|defaultvalue) <name> of
settings.default
```

Example:

```
# get value Network.RDP.port of settings.default

3389
```

Set a value of a default setting:

```
# set value Network.RDP.port of settings.default to
3389
```

8.3.4.9 Dataset: settings.profiles

This dataset handles profiles itself, not the settings associated to a profile (See settings.profile).

Get a list of all profiles:

```
# get settings.profiles

3 default 0

4 login 1
```

The result contains the profile ID, the profile name and the passive flag (1 … passive, 0 … not passive).

Create a profile:

```
# add profile of settings.profiles <new profile
name> to <passive flag>
```

Example:

```
# add profile of settings.profiles testprofile to 0
```

8.3.4.10 Dataset: settings.profile

Get a list of all profile settings:

© 2006-2007 Thinstuff s.r.o

```
# get settings.profile name:profilename
```

The "name:" is optional in all actions to settings.profile, it is also allowed to write:

```
# get settings.profile profilename
```

Query a specific feature of a setting:

```
# get (id|name|type|isset|islist) <name> of
settings.profile name:profilename

# get (level|value|defaultvalue) <name> of
settings.profile name:profilename
```

Example:

```
# get value Session.maxWidth of settings.profile
name:login

1600
```

Set a value of a profile setting:

```
# set value Session.maxWidth of settings.profile
name:login to 1200
```

9 Licensing, Upgrading and Support

9.1 Licensing

When you first install your Thinstuff LX Server it contains a special license for "Service Mode". This license allows you to use the web interface but does not allow any RDP connections to your server. To use your server, you will need a server license. If you do not already own such a license, you can get one from http://www.thinstuff.com/licensing/ .

Place your licenses in the folder **`/opt/thinstuff/rdpserver/licenses`**. This can be done conveniently via the web based configuration and management interface. Just go to "Cluster Status" -> "Licenses" and upload your files via the dialog provided to the right.

When you first receive your licenses, they are not activated. This means that they will work on any computer, but only for a limited time (usually one month). You have to activate your licenses for a particular computer to receive the final license which is valid for the full duration. To activate a license, go to our licensing page http://www.thinstuff.com/licensing/. Once you log in with your username and password, you will see the licenses you bought for each product, and an activation link next to them. Click the link and follow the instructions on the webpage to activate your licenses. Once the license is activated it will only work on the PC you activated it on. If you need to use the license on a different

PC please contact us and we can provide you with a possibility to redo the activation.

9.2 Upgrading

To upgrade Thinstuff LX Server all you need to do is download a new license and install it as described above. Only one product can be active at a given time, so it is not necessary to remove the old licenses. To go back to the previous version, just remove the newer license from the licensing folder.

If you own licenses for one of our products, you can upgrade to new versions without paying the full price. Go to our licensing page http://www.thinstuff.com/licensing/ and log in using your username and password. You will see a list of products you have already bought and activated. Just select one and click the corresponding upgrade link to begin the upgrade process.

Please note that you need to activate your licenses before you can upgrade them. It is not possible to upgrade licenses which are not yet activated for a PC.

10 How-to

10.1 Profile Questions

How do I change which window manager or desktop environment a specific profile uses?

1. Use the Configuration Wizard, or perform the following steps:
2. Go to "Settings" -> "Advanced Settings".
3. Select the profile you want to modify (if the page does not load automatically, hit the "Change Profile" button).
4. Change "Applications.session.command" to the command to execute your desired desktop environment. Some choices include:
   a. **`/opt/thinstuff/rdpserver/bin/twm`** – Use the included "twm" window manager (default value).
   b. **`startkde`** – Start a KDE session.
   c. **`gnome-session`** – Start a GNOME session.
   d. **`icewm-session`** – Start the IceWM window manager.

   NOTE: Do not set the session command to a shell script, unless that script will run for the whole duration of the session. If a session command is given, then the session will terminate as soon as the started program ends.

© 2006-2007 Thinstuff s.r.o

How do I create a profile with specific values for a certain user/group/hostname?

1. Go to "Settings" -> "Profiles".
2. Select the profile you want to base your new profile on (if the page does not load automatically, hit the "Change Profile" button).
3. Enter a new profile name.
4. Check "Copy from selected" if you want to copy the values from the selected profile. Otherwise every value will be set to the default values.
5. Change the value for "Match.users.enable" to true to enable matching specific user names (analogous use "Match.groups.enable" or "Match.hosts.enable" for groups or hostnames).
6. Edit the value "Match.users.values" and add the usernames you want to match.
7. Edit the other profile settings to the desired values.
8. Test it. You should now get the specified profile settings when connecting with the given user.

How do I prevent a profile from creating more than one session?

1. Go to "Settings" -> "Profiles".
2. Select the profile you want to modify (if the page does not load automatically, hit the "Change Profile" button).
3. Change the view level to "Level 1 (Advanced)".
4. Change "Session.reconnectToConnected" to "true".

10.2 Session Questions

How can I find the IP address of the client who created a session?

You can use the THINSTUFF_TOUCH_SESSION_CLIENT_IP environment variable. If the environment variable is not accessible to you, you can use the session file to get the same information. Please see chapter 4.2 for more information and caveats.

How do I create a session that uses XDMCP to connect to a running display manager?

1. Go to "Settings" -> "Profiles".
2. Select the profile you want to modify (if the page does not load automatically, hit the "Change Profile" button).
3. Change "Applications.session.command" to "-query my.xdmcp.host" where my.xdmcp.host is the address of the machine the display

© 2006-2007 Thinstuff s.r.o

manager runs on (use localhost if it is the same machine the terminal server runs on).

How can I create a session that does not start anything?

1. Go to "Settings" -> "Profiles".
2. Select the profile you want to modify (if the page does not load automatically, hit the "Change Profile" button).
3. Clear the "Applications.session.command" setting, so it is empty. This session will end once the associated X11 Server is terminated. Currently there is no automated way of finding out the display number of the newly created session, you will have to use the web interface.

   NOTE: Do not set the session command to a shell script, unless that script will run for the whole duration of the session. If a session command is given, then the session will terminate as soon as the started program ends.

10.3 Authentication Questions

How do I set up PAM so I can authenticate against Microsoft Active Directory Service ?

You can use the following script as a starting point for your PAM configuration file. By default this is **`/etc/pam.d/touch-rdp`**

```
# Read environment variables from /etc/environment
# and/etc/security/pam_env.conf.
auth     required     pam_env.so


# Standard Un*x authentication.
auth     sufficient   pam_unix.so likeauth nullok
auth     sufficient   pam_krb5.so \
   ccache=/tmp/krb5cc_%u use_first_pass \
   forwardable debug realm=my.domain.com
auth     required     pam_deny.so


# Standard Un*x authorization.
account  sufficient   pam_unix.so
account  required     pam_krb5.so


# Standard Un*x session setup and teardown.
```

```
session  required     pam_unix.so
session  required     pam_krb5.so
session  optional     pam_foreground.so


# Print the message of the day upon successful
# login.
session  optional     pam_motd.so


# Print the status of the user's mailbox upon
# successful login.
Session  optional     pam_mail.so standard noenv


# Set up user limits from /etc/security/limits.conf
Session  required     pam_limits.so


# Standard Un*x password updating.
password required     pam_unix.so nullok \
   obscure min=4 max=8 md5
```

10.4 Virtual Channel Questions

If you have problems with sound, please try the following:

1. Make sure sound is enabled on the RDP client
2. Make sure sound is enabled for your session
3. If you are using ESD, then try to modify the ESD mode in the configuration wizard.
4. If your system has a native pulse-audio server, make sure it is turned off. LX Server starts its own.

11 Compatibility

11.1 RDP Clients

The server is tested to be compatible with the following RDP Clients:

- rdesktop 1.3.1
- rdesktop 1.4
- rdesktop 1.5
- Microsoft RDP Client 5.1.2600.0 (Windows XP)

- Microsoft RDP Client 5.1.2600.1160 (Windows XP, SP1)
- Microsoft RDP Client 5.2.3790 (Windows XP, SP2)
- Microsoft RDP Client 6.0 (Windows Vista)
- Microsoft RDP Clients for Mac OS X
- Wyse S10

The following clients work, but because of certain incompatibilities might run slower than expected:

- Microsoft RDP Client 5.0 (Windows 2000)
- Microsoft RDP Client on Windows CE 5.0

11.2 Hardware and Software

The package will run on all 32-bit x86 Linux based distributions with 32-bit glibc 2.2.5 or higher, a 32-bit PAM library (pam.so) and kernel versions 2.4.x or 2.6.x.

On 64-bit Linux systems which support 32-bit applications (Opteron, Athlon 64, …) it might be required to install compatibility libraries.

For installation a bash compatible shell and bzip2 are required.

The minimum hardware requirements are:

- Intel Pentium III 1 GHz or compatible
- 256 MB RAM
- ~ 200 MB of hard disk space

12Trademarks

The GNOME logo and GNOME name are registered trademarks of GNOME Foundation in the United States or other countries.

KDE® is the registered trademark of KDE e.V.

Linux® is the registered trademark of Linus Thorwalds in the U.S. and other countries.

Windows® and Active Directory® are the registered trademarks of Microsoft Corporation in the United States and/or other countries.

© 2006-2007 Thinstuff s.r.o

Appendix A – Settings Descriptions

Setting	Level	Profile	Description
ApplicationLauncher.xservercheck.iorTimeout	2	Y	Specifies the CORBA timeout for checking Xxpt
ApplicationLauncher.xservercheck.retries	2	Y	Specifies the number of Xxpt checks done
ApplicationLauncher.xservercheck.sleep	2	Y	Specifies the time in milliseconds [ms] between the checks if Xxpt has been started properly
Applications.authclient.command	2	Y	Specifies the path to the authentication client binary
Applications.authclient.env	2	Y	A list of environment variables used for starting the authentication client
Applications.authclient.parameters	2	Y	The parameters passed to the authentication client binary
Applications.authclient.workingdir	2	Y	Specifies the working directory for starting the authentication client
Applications.locale.command	2	Y	Specifies the command for setting the locale. This can be any program which accepts a locale specification in one of two forms. Either -i <LCID> or -l <locale name>. LCID is a Windows Locale ID in the form of a 32bit hexadecimal number. Locale name is an ISO locale name in the form of e.g. en, de, de_DE
Applications.locale.env	2	Y	A list of environment variables used for starting the locale application
Applications.locale.parameters	2	Y	Additional parameters to pass to the locale application
Applications.locale.workingdir	2	Y	Specifies the working directory for starting the locale application
Applications.session.command	0	Y	Specifies the command to the session application binary (e.g. kde, gnome, icewm,...). **Important:** see the Applications.session.env configuration setting to make sure the enviroment matches your executables.
Applications.session.env	1	Y	A list of environment variables used for starting the session application. When using your own window managers please make sure to use your system environment settings. **Default value:** PATH=${PATH:+$PATH:}/opt/thinstuff/rdpserver/bin
Applications.session.parameters	0	Y	The parameters passed to the session application
Applications.session.workingdir	0	Y	Specifies the working directory for starting the session application
Applications.sessionFile.command	2	Y	Specifies the command used to manipulate the session files.
Applications.sessionFile.env	2	Y	A list of environment variables used for starting the session file application
Applications.sessionFile.parameters	2	Y	Additional parameters to pass to the session file application
Applications.sessionFile.workingdir	2	Y	Specifies the working directory for starting the session file application
Applications.xauth.command	2	Y	Specifies the command used to manipulate the .Xauthority file. This can be any program compatible to xauth
Applications.xauth.env	2	Y	A list of environment variables used for starting the xauth application
Applications.xauth.parameters	2	Y	Additional parameters to pass to the xauth application
Applications.xauth.workingdir	2	Y	Specifies the working directory for starting the xauth application
Applications.xserver.command	2	Y	Specifies the path to the Xxpt binary

© 2006-2007 Thinstuff s.r.o

Setting	Level	Profile	Description
Applications.xserver.env	2	Y	A list of environment variables used for starting Xxpt
Applications.xserver.parameters	2	Y	The parameters passed to the Xxpt executable (e.g. font paths, special backgrounds,...)
Applications.xserver.user	2	Y	The user to run Xxpt as
Applications.xserver.workingdir	2	Y	Specifies the working directory for Xxpt
Match.groups.enable	0	Y	This setting controls if this profile is matched by comparing group names
Match.groups.values	0	Y	A list of groups who are used to select this profile
Match.hosts.enable	0	Y	This setting controls if this profile is matched by comparing client hostnames
Match.hosts.values	0	Y	A list of client hostnames which are used to select this profile
Match.users.enable	0	Y	This setting controls if this profile is matched by comparing user names
Match.users.values	0	Y	A list of users who are used to select this profile
Network.ConnectionForwarding. socketrange.max	1	N	This is the end of the socketrange where the tcpforwarder will allocate ports for tcp forwarding to the X servers. NOTE: you will need room for at least one socket per connection you want to run simultaneously.
Network.ConnectionForwarding. socketrange.min	1	N	This is the start of the socketrange where the tcpforwarder will allocate ports for tcp forwarding to the X servers. NOTE: you will need room for at least one socket per connection you want to run simultaneously.
Network.ConnectionForwarding. timeout.sec	2	N	**INTERNAL:** this is the tcp forwarder thread socket finished/error/exception checking interval (the seconds part)
Network.ConnectionForwarding. timeout.usec	2	N	**INTERNAL:** this is the tcp forwarder thread socket finished/error/exception checking interval (the microseconds part)
Network.RDP.port	0	N	The port to listen on for incoming RDP client connections
RdpServer.BitmapCache. cacheHistorySize	1	Y	The cache history size determines how many tiles the server keeps in memory, to determine usage frequency. A bigger history size will result in tiles being kept longer in cache before being evicted by newer tiles. Smaller sizes will allow the cache to evict tiles faster, resulting in better performance when the cached tiles become obsolete often and quickly (eg: during browsing). This also affects memory performance, and is affected by the tile size below. Bigger tile sizes need smaller caches to be effective. **Possible Values:** [1 .. 2^32-1] **Recommended Values:** [1024 .. 16384] **Default Value:** 16384
RdpServer.BitmapCache. limitCacheSize	2	Y	limitCacheSize can be used to artificially limit the cache size used on the client. Usually it is not a good idea to use this, unless certain clients refuse to work, or memory limits on the client are extremely tight. **Possible Values:** [0 (off), 1 .. 2^32-1] **Recommended Value:** 0 (off) **Default Value:** 0 (off)

© 2006-2007 Thinstuff s.r.o

Setting	Level	Profile	Description
RdpServer.BitmapCompressor. enableRLECompression	1	Y	Allow RLE compression to be used for bitmap data. RLE Compression is performed before and independently of RDP compression. Usually there is no reason to turn this off, but in certain environments where bandwidth does not matter (e.g: LANs) not using compression might improve CPU usage and latency. Note however that because of the increased strain on the RDP compressor, encryption and/or the network itself, the opposite may be true, your mileage may vary. **Possible Values:** [false, true] **Recommended Value:** true **Default Value:** true
RdpServer.BitmapRequest. cacheLimit1	2	Y	Updates smaller than this in a single direction will always be sent uncached, since sending a full tile for them is unlikely to bring any gain. **Possible Values:** [0 (off), 1.. 2^32-1] **Recommended Values:** [1 .. tileSize/4] **Default Value:** 4
RdpServer.BitmapRequest. cacheLimit2	2	Y	Updates with fewer pixels than this in total will always be sent uncached, since sending a full tile for them is unlikely to bring any gain. **Possible Values:** [0 (off), 1.. 2^32-1] **Recommended Values:** [1 .. tileSizeX*tileSizeY/16] **Default Value:** 256
RdpServer.BitmapRequest. sendBoundsFactor	2	Y	Complex regions are sent as a series of update rectangles if the sum of areas of the rectangles, compared to the area of the bounding rectangle is lower than this factor, otherwise it is sent by sending the bounding rectangle. **Possible Values:** [0 .. 1] **Recommended Values:** [0.7 .. 0.9] **Default Value:** 0.8
RdpServer.Connection. desiredFlushSize	2	Y	Preferred packet size. Smaller packets result in faster responses from the server at the expense of bandwidth efficiency. Especially on very slow connections (ISDN) lower values may greatly increase the perceived performance for interactive work (office, ...). **Possible Values:** [0 .. 16384] **Recommended Values:** [1024 .. 8192] **Default Value:** 8192
RdpServer.Connection. enableFastCompression	2	Y	Enabling this flag results in a slightly different hash algorithm to be used in the RDP compressor. This results in about 5-10% worse compression quality, but improves compression speed by 5-10%. **Possible Values:** [false, true] **Recommended Value:** false **Default Value:** false

© 2006-2007 Thinstuff s.r.o

Setting	Level	Profile	Description
RdpServer.Connection. enableRdp2Compression	1	Y	Allow the improved compression of newer RDP clients to be used. Usually you always want this on since the newer compression gives better performance and better compression quality (up to 30%). Turn this off, if the client wrongly reports support for the new compression although it is not present (currently no such client is known). Ignored if enableRdpCompression is false. Note that even if set to true, the server will not use compression if it is not supported by the client, so it is safe to leave this on true. **Possible Values:** [false, true] **Recommended Value:** true **Default Value:** true
RdpServer.Connection. enableRdpCompression	0	Y	Allow compression to be used. Compression gives a big improvement in bandwidth and you usually want compression on. In certain environments where bandwidth does not matter (e.g: LANs) not using compression might improve CPU usage and latency. Note however that because of the increased strain on the RDP encryption and/or the network itself, the opposite may be true, your mileage may vary. Note that even if set to true, the server will not use compression if it is not supported by the client, so it is safe to leave this on true. **Possible Values:** [false, true] **Recommended Value:** true **Default Value:** true
RdpServer.ImageBuffer. allowSplitting	1	Y	Allow splitting of tiles. This allows splitting of tiles along a horizontal line when updates do not need a full tile to be sent. Tiles are re-merged later automatically. This can improve bandwidth by sending less image data, but more tiles are generated which leads to worse cache usage. Overall the gain is usually higher for typical desktop work when turning this on. Scrolling and internet browsing might benefit from this setting. **Possible values:** [false, true] **Recommended value:** true **Default value:** true
RdpServer.ImageBuffer. hashMultiplier	2	Y	Hash base and multipliers. Subhashes are calulcated as ((base + array[0])*multiplier + array[1])*multiplier ... Hashes are calculated as (subhash[0]*multiplier+subhash[1])*multiplier ... multipliers should result in good distribution of bits (e.g: prime numbers) **Possible values:** [1 .. 2^32-1] **Recommended values:** any prime number **Default Values:** 31 (multiplier), 2166136261 (base)
RdpServer.ImageBuffer. subHashBase	2	Y	The subhash base for hash calculation (see hashMultiplier for more details)
RdpServer.ImageBuffer. subHashMultiplier	2	Y	The subhash multiplier for hash calculation (see hashMultiplier for more details)
RdpServer.ImageBuffer.tileSizeX	2	Y	Initial X tile size. X size is fixed, Y size can vary from [1 .. tileSizeY]. Smaller tile sizes usually result in faster transmission, while large sizes result in a better cache usage. **Possible values:** [1 .. 64] **Recommended values:** [32, 48, 64] **Default values:** 64x64

© 2006-2007 Thinstuff s.r.o

Setting	Level	Profile	Description
RdpServer.ImageBuffer.tileSizeY	2	Y	Initial Y tile size. X size is fixed, Y size can vary from [1 .. tileSizeY]. Smaller tile sizes usually result in faster transmission, while large sizes result in a bigger cache usage. **Possible values:** [1 .. 64] **Recommended values:** [32, 48, 64] **Default values:** 64x64
RdpServer.LinesRequest.enable	1	Y	Line orders do not work on RDP6 clients and cause visual artifacts on other clients, therefore line orders are disabled by default. You can use this setting to enable them. **Possible Values:** [false, true] **Recommended Value:** false **Default Value:** false
RdpServer.LinesRequest.extendLines	1	Y	The RDP protocol does not draw the endpoints of a line, while the X server does. This leads to minor graphical inconsistencies. Order translation tries to alleviate this by extending lines by one pixel so that the resulting RDP operation should exhibit the same behavior as the original X request. However, rdesktop clients up to version 1.4.1 do ignore this minor detail and produce lines which include the last point, staying true to the original X method of drawing things. In this case the above mentioned fix causes lines to overshoot by one pixel. rdesktop clients should be autodetected, but if this does not work correctly you can try to change this setting to manually disable the line extension. **Possible Values:** [false, true] **Recommended Value:** true **Default Value:** true
RdpServer.MTU	2	Y	The maximum transferable unit within the RDP protocol translation. Adjust this setting to match your transport layer (e.g. Ethernet, internet routing,...)
RdpServer.ProtocolTracer. fontAliasThreshold	1	Y	Allow antialiased fonts to be sent as aliased fonts. RDP has no notion of antialiased fonts, therefore antialiased text must be sent as bitmaps if pixel perfect representation is desired. It is however possible to convert antialiased fonts back to aliased fonts, resulting in less bandwidth usage at the expense of image quality. The following setting controls how and if fonts are converted. Note that higher numbers will result in fonts to appear lighter, while lower ones make them appear bolder. **Possible Values:** [0 (off), 1 .. 255] **Recommended Values:** [0 (off), 112 .. 140] **Default Value:** 0

© 2006-2007 Thinstuff s.r.o

Setting	Level	Profile	Description
RdpServer.Translator.queueSize	2	Y	The maximum number of requests (pseudo RDP operations) to be queued between the protocol tracer and the actual translator. Lower values will make the session block faster if the network connection is slow (or start spoiling more aggressively), while higher values give the server more time to ease out short bottlenecks in bandwidth. Lower values will produce tighter real-time behavior at the expense of bandwidth and/or update frequency, while higher values will result in a general smoother experience at the expense of RAM and responsiveness. **Possible Values:** [2 .. 2^32-1] **NOTE:** do not set to 0 or 1 ! **Recommended Values:** [2 (syncronized mode), 64 (multimedia) .. 1024 (office)] **Default Value:** 64
RdpServer. alwaysSendTrueCursorKeys	2	Y	Some applications (most notably Oracle Forms) seem to have problems with numpad cursor keys. They do not react to xmodmap redefinition of those keys (probably use actual scancode) and some clients (e.g: Windows CE 5.0 on Symbol PDA) send cursor keys as numpad cursor keys. By setting this value to true, the RDP server redefines scancodes for these keys to always behave like actual cursor keys. Use with caution, and don't tamper with it if your setup is working as intended as it might destroy normal operation of the numpad area. **Possible Values:** [false, true] **Recommended Value:** false **Default Value:** false
RdpServer.defaultBellFrequency	1	Y	Default setting for the system beep frequency. If no other parameter is set by a program, then this value will be used.
RdpServer.defaultBellTime	1	Y	Default setting for the system beep bell time. If no other parameter is set by a program, then this value will be used.
RdpServer.enableBitmapCache	0	Y	Allow the usage of the bitmap cache. Usually you always want to enable this, since it provides great increases in performance. Disable this if the cache is not working correctly, or if you have special needs (e.g: multimedia applications in a LAN environment) **NOTE:** this also disables any usage of the ImageBuffer
RdpServer.verifyDisconnect	0	Y	Bring up the "Do you really want to disconnect?" dialog when trying to close a windows client. **Possible values:** [false, true] **Recommended value:** true **Default value:** true
Security.Authentication.PAM-Service	1	N	Name of the PAM service used to perform user authentication.
Security.Authentication. authenticationProfile	1	N	The configuration profile to use during the logon process
Security.Authentication. authenticationUsername	1	N	The system username to use for starting applications for the logon process
Security.Authentication.caseSensitive	1	N	Specifies if your authentication service is case sensitive or not. Normal Linux system authentication is case sensitive, so "user", "USER" and "User" are three different accounts. Only set this to false if you are sure your authentication is not case sensitive. **NOTE:** Usernames for profile matching are still case sensitive and must be written exactly as they appear in the user list.

© 2006-2007 Thinstuff s.r.o

Setting	Level	Profile	Description
Security.Authentication. performEarlyAuthentication	1	N	Specifies if the terminal server should check the username and password directly provided by the clients (and thus maybe allow them to logon without ever having to enter a password in the logon dialog)
Security.Authentication. performLateAuthentication	1	N	Specifies if the terminal server should show a logon dialog if early authentication (sending username and password with the client) either failed or was disabled. If this is false and early authentication fails the connection will be closed
Security.RDP.CACert	2	N	The certification authority certificate (CA cert) to use for the encryption process
Security.RDP.ClientCert	2	N	The client certificate to use for RDP encryption. This certificate is sent to all clients
Security.RDP.CryptoVersion	2	N	RDP cryptography version, the only valid value is 5
Security.RDP.KeyLength	2	N	The key length for the symmetric encryption in bytes. The only valid value is 16
Security.RDP.ProtocolVersion	2	N	RDP protocol version, the only valid value is 5
Security.RDP.ServerCert	2	N	The server certificate to use for RDP encryption
Security.RDP.ServerKey	2	N	The server private key to use for RDP encryption
Session.Displayallocation.max	1	Y	Specify the upper limit for the range of display numbers to use for sessions in this profile. **Possible values:** [0 .. 65535] **Recommended value:** at least 100 higher than min **Default value:** 65536
Session.Displayallocation.min	1	Y	Specify the lower limit for the range of display numbers to use for sessions in this profile. **Possible values:** [0 .. 65535] **Recommended value:** at least 100 lower than max **Default value:** 100
Session.changeKeyboard	0	Y	Enable this setting to set the keyboard layout to the keyboard layout of the connecting client. Disable this if you want all users to use the keyboard layout provided by the host.
Session.ctypeFromKeyboard	1	Y	Enable this setting to set the character handling locale for a session based on the requested keyboard layout at connect time. This ensures that dead-key composition, capitalization, etc. work correctly. Disable this if you want all users to use the locale provided by the host. Enabling this effectively sets the "LC_CTYPE" environment variable. **NOTE:** A wrong locale setup may prohibit keyboard layouts from working correctly. Disabling this will also disable Session.languageFromKeyboard.
Session.keepLanguageFromLogin	1	Y	If enabled the language selected in the login dialog will be used for the new session, otherwise the language of the session is the language of the system the client runs on.
Session.languageFromKeyboard	0	Y	Enable this setting to set the system language for a session based on the requested keyboard layout at connect time. This makes locale aware programs (Gnome, KDE, OpenOffice, ...) display menus and alerts in the right language. Disable this if you want all users to use the language provided by the host. Enabling this effectively sets the "LANG" environment variable.
Session.matchPerClienthost	2	Y	Enable this setting if existing sessions should be reconnected by matching the client hostname

© 2006-2007 Thinstuff s.r.o

Setting	Level	Profile	Description
Session.matchPerUser	2	Y	Enable this setting if existing sessions should be reconnected by matching the username
Session.maxDepth	0	Y	Specify the maximum color depth a client can use. Warning: 24 bit color depth may result in higher CPU usage if clients do not actually connect in 24 bit mode. It is recommended that 16 bit mode is used unless 24 bit mode is explicitly needed. **Possible values:** 8, 16, 24 **Recommended values:** 16 **Default value:** 16
Session.maxHeight	0	Y	Specify the maximum height of the resolution a client can use. Note that very high values will result in high memory usage of sessions, even if the client is connected with a much lower resolution. **Possible values:** [1 .. 65535] **Recommended values:** 480, 600, 768, 1024, 1200, 1536 **Default value:** 1200
Session.maxWidth	0	Y	Specify the maximum width of the resolution a client can use. Note that very high values will result in high memory usage of sessions, even if the client is connected with a much lower resolution. **Possible values:** [1 .. 65535] **Recommended values:** 640, 800, 1024, 1280, 1600, 2048 **Default value:** 1600
Session.reconnectToConnected	1	Y	If enabled the session chooser will also consider sessions with connections as eligible when reconnecting a client. **NOTE:** since the chooser does not get shown when only a single choice is available this means that a user is typically limited to a single session (every further connection will join the old one automatically).
Session.sessionFiles	1	Y	Specify a path where to place session files. A session file contains the definitions of the THINSTUFF_TOUCH_XXX environment variables and is named by the display number. This can be used if the normal environment variables are not usable for some reason (e.g: when -query is used). **NOTE:** This script is executed in the security context of the session user, so make sure the directory exists and is writable by this user. You can use /opt/thinstuff/rdpserver/var/sessions for this purpose. The session files are created by the command specified in Applications.sessionFile.command. You can modify this script to change the content of the session files. The command is given the directory as a single command line parameter. The session will block until this command is written.
Session.timeout	0	Y	The timeout in seconds until a running session without connected clients is kept alive before killing it (-1 means forever, 0 means that the session is killed after the last client disconnects)

© 2006-2007 Thinstuff s.r.o